Mastering data protection and compliance

Introductions

Learning Outcomes Overview

Image source: Microsoft 365 content library

New Technologies

Explain what the UK GDPR considers to be "new technologies" and what this means in practice.

PECR Compliance

Identify when your marketing activity needs to comply with PECR as well as the UK GDPR.

Documentation

Understand what documentation you should be have in place to demonstrate your compliance with these requirements.

Risk Mitigation

Apply effective risk mitigation measures for marketing and AI related compliance risks.

PRIVACY PROTECT GROUP
SECURING YOUR DATA, PROTECTING YOUR PRIVACY

This session will equip you with the knowledge required to understand the essentials of
arketing communications and cookie technologies), how to safely use Artificial Intelligence and New Technologies, and how to demonstrate compliance through documentation and risk management.

Following this session, you will be able to:

- **Explain** what the UK GDPR considers to be "new technologies" and what this means in practice.
- **Identify** when your marketing activity needs to comply with PECR as well as the UK GDPR.
- **Understand** what documentation you should be have in place to demonstrate your compliance with these requirements.
- **Apply** effective risk mitigation measures for marketing and AI related compliance risks.

Image source: from Bing

Innovative Technologies

PRIVACY PROTECT GROUP
SECURING YOUR DATA, PROTECTING YOUR PRIVACY

Let’s start with innovative technologies

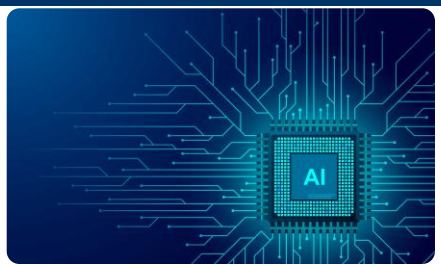
What does 'Innovative Technologies' mean?

Examples of processing using innovative technology include:

- Artificial intelligence, machine learning, and deep learning;
- Connected and autonomous vehicles;
- Intelligent transport systems.

Examples of processing using innovative technology include:

- smart technologies (including wearables);
- market research involving neuro-measurement (e.g. emotional response analysis and brain activity);
- some 'internet of things' applications, depending on the specific circumstances of the processing.



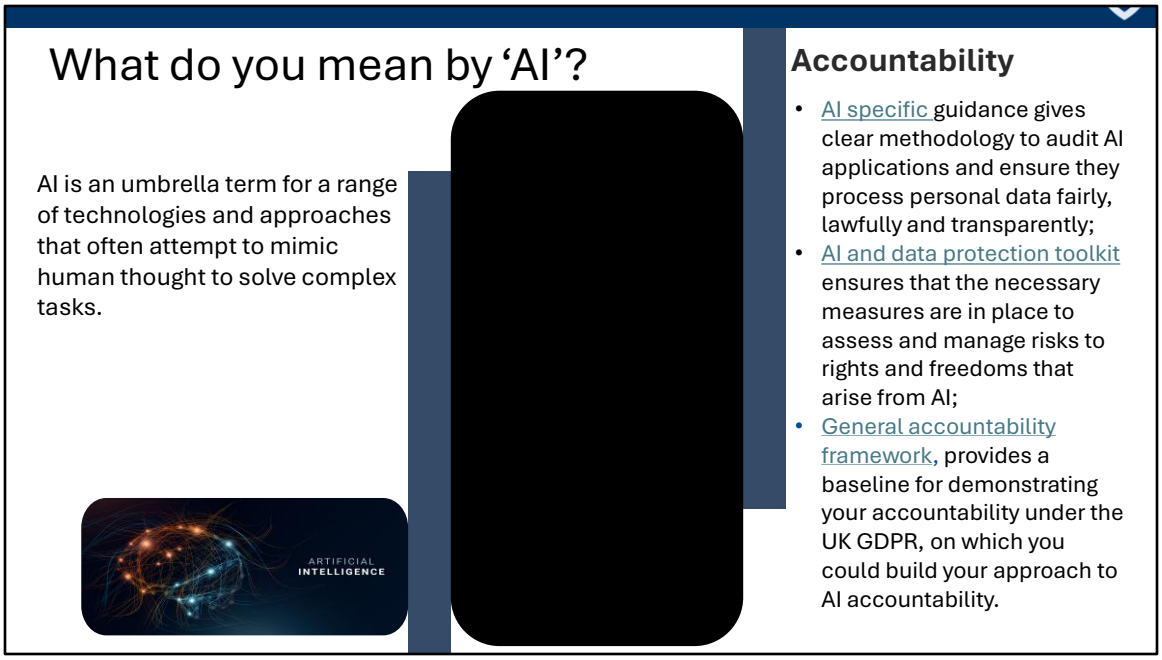
Recital 91 of the UK GDPR says innovative technology concerns new developments in technological knowledge in the **world at large** and its use can trigger the need to carry out a Data Protection Impact Assessment (DPIA) as outlined in Article 34 of the UK GDPR. This is because using such technology can involve novel forms of data collection and use, possibly with a high risk to individuals' rights and freedoms.

Processing which uses innovative technologies could be the likes of:

- **Machine learning (ML)** which is a set of techniques and tools that allow computers to 'think' by creating mathematical algorithms based on accumulated data.
- **Deep learning** which is a subset of machine learning where systems 'learn' to detect features that are not explicitly labelled in the data.
- **Intelligent transport systems:** which involves the car communicating with other vehicles, warning of any obstacles down the road etc.
- **Internet of things:** the network of physical objects "things" that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet e.g. cars, toothbrushes, vacuum robots, etc.

- **Smart technologies** such as smart watches, aura rings etc.

However, it is not just cutting-edge technology that might be classed as innovative. If as a business, you **implement existing technology in a new way**, this could result in high risks, that unless a DPIA is done, you may not be identified and dealt with. The personal and social consequences of deploying a new technology may be unknown, and a DPIA can help you to understand and control such risks.



So AI is an innovative technology, but what exactly is AI?

The umbrella term ‘AI’ has become a standard industry term for a range of technologies. One prominent area of AI is ‘machine learning’ (ML), which is the use of mathematical techniques to create (often complex) statistical models using (typically) large quantities of data. Those models can be used to make classifications or predictions about new data points. While not all AI involves ML, most of the recent interest in AI is driven by ML in some way, whether in image recognition, speech-to-text, or classifying credit risk.

AI is not one thing. There are multiple types of AI, each defined by how it learns, what it does, and the value it creates.

Different types of AI solve different problems:
- generative AI *creates*,
- predictive AI *forecasts*,
- assistive AI *supports work*, and
- agentic AI *performs tasks autonomously*.

Large language models (LLMs) and multimodal systems now dominate the modern workplace, particularly in knowledge work.

Agentic AI and multimodal AI are accelerating rapidly, reshaping how organisations evaluate AI capabilities.

Choosing the right type of AI starts with identifying a business need, mapping it to the correct AI category, selecting appropriate model technology, and scaling responsibly.

The ICO has released guidance which covers what they think is best practice for data protection-compliant AI, as well as how they interpret data protection law as it applies to AI systems that process personal data. There is no penalty if you fail to adopt good practice recommendations, as long as you find another way to comply with the law.

In addition to documenting your assessment in the DPIA, you are encouraged to utilise the AI and data protection toolkit to identify and manage risks. This could then be supported by the general accountability framework for general compliance. All of this builds on what we've been discussing in previous sessions in terms of keeping your contracts in date and under review, ensuring your privacy notices are fully documented and that you know what risk appetite you work within.

How should we approach AI governance?

How do we ensure:
- transparency in AI?
- lawfulness in AI?
- fairness in AI?

What do we need to know about accuracy and statistical accuracy?

What security risks does AI introduce?

How do we ensure individual rights in our AI systems?

AI can bring benefits to organisations and individuals, but there are risks too.

If used well, AI has the potential to make organisations more efficient, effective and innovative. However, AI also raises significant risks for the rights and freedoms of individuals, as well as compliance challenges for organisations. You cannot delegate these issues to data scientists or engineering teams. Your senior management, including DPOs, are also accountable for understanding and addressing them appropriately and promptly (although overall accountability for data protection compliance lies with the business owner as the Controller).

AI governance is essentially the process of having a structured, considered, and documented approach to deploying and using AI tools.

To manage the risks to individuals that arise from processing personal data in your AI systems, it is important that you develop a mature understanding of fundamental rights, risks, and how to balance these and other interests. Ultimately, it is necessary for you to:
- assess the risks to individual rights that your use of AI poses;
- determine how you will address these; and

- establish the impact this has on your use of AI.

This is a complex task, which can take time to get right. However, it will give you, as well as the ICO, a fuller and more meaningful view of your risk positions and the adequacy of your compliance and risk management approaches.

Some of the things you should be assessing to identify risks, are:

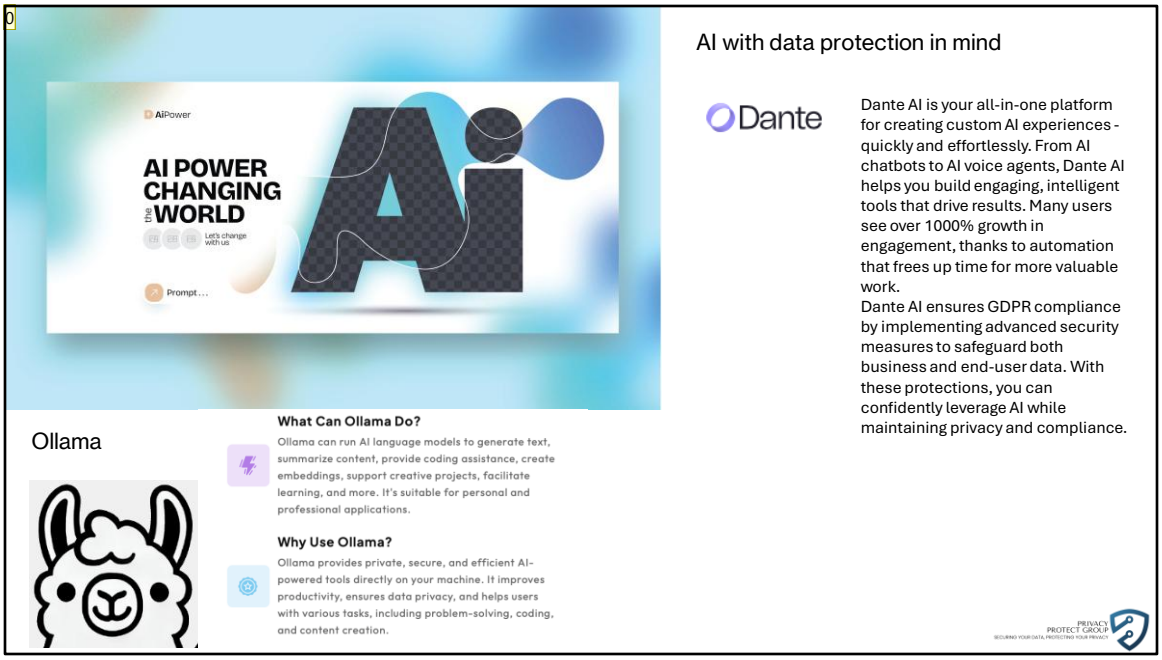
- **Transparency and lawfulness:** You need to be transparent about how you process personal data in an AI system. You need to decide your lawful basis for processing personal data in the context of AI development and/or deployment. The development and deployment of AI systems involve processing personal data in different ways for different purposes. You must break down and separate each distinct processing operation, Different lawful bases may apply depending on your particular circumstances. At the same time, you must remember that:
    - it is **your responsibility** to decide which lawful basis applies to your processing;
    - you must always choose the lawful basis that **most closely reflects the true nature of your relationship** with the individual and the purpose of the processing;
    - you should make this determination **before** you start your processing;
    - you should **document** your decision;
    - you **cannot swap** lawful bases at a later date without good reason;
    - you must **include your lawful basis** in your privacy notice (along with the purposes); and
    - if you are processing **special categories of data** you need **both** a lawful basis **and** an additional condition for processing.
- **Accuracy:** It is important to note that the word 'accuracy' has a different meaning in the contexts of data protection and AI. Accuracy in data protection is one of the fundamental principles, requiring you to ensure that personal data is accurate and, where necessary, kept up to date. It requires you to take all reasonable steps to make sure the personal data you process is not 'incorrect or misleading as to any matter of fact' and where necessary, is corrected or deleted without undue delay. For AI the term 'statistical accuracy' is used to refer to the accuracy of an AI system itself. Data protection's **accuracy principle** applies to all personal data, whether it is information about an individual used as an input to an AI system, or an output of the system. However, this does not mean that an AI system needs to be 100% **statistically accurate** to comply with the accuracy principle.
- **Fairness:** Fairness in data protection is not just about discrimination. It is important to note, particularly in AI, that data protection's specific requirements and considerations work together to ensure your AI systems

process personal data fairly and lead to fair outcomes. In addition to those already covered, you need to make sure you're considering individual rights and how these can still be exercised where their data is used in AI tools.

- **Security:** There is no 'one-size-fits-all' approach to security. The appropriate security measures you should adopt depend on the level and type of risks that arise from specific processing activities.

  Using AI to process any personal data has important implications for your security risk profile, and you need to assess and manage these carefully. Some implications may be triggered by the introduction of new types of risks, eg attacks on machine learning models which may lead to personal data of the people who an AI system was trained on inadvertently being revealed, in some cases, even by the outputs of the system itself.

  It is normally assumed that the personal data of the individuals whose data was used to train an AI system cannot be inferred by simply observing the predictions the system returns in response to new inputs. However, new types of privacy attacks on ML models suggest that this is sometimes possible.
- **Individuals' right:** Under data protection law individuals have a number of rights relating to their personal data. Within AI, these rights apply wherever personal data is used at any of the various points in the development and deployment lifecycle of an AI system. This therefore covers personal data:
  - contained in the training data;
  - used to make a prediction during deployment, and the result of the prediction itself; or
  - that might be contained in the model itself;
  - that is input into the model when using it e.g. what you prompt an AI tool with.



So we've touched on the innovative technologies, but what about AI tools that feed into profiling and automated decision making in the context of marketing activity?

AI is often used in marketing in the following ways:

- Sentiment analysis on social media to aggregate positive and critical product reviews
- Automating competitor intelligence reports to stay up to date with what rival brands are doing (this is often to improve the ROI of your marketing campaigns with better targeting)
- AI workflows to write creative copy, helping you keep up with the internet's incessant demand for content (i.e. search engine optimisation).
- Video editing and content creation
- Automating, anonymising and presenting reports
- Ad creation automation

This means that the tools you rely on to administer mailing lists, schedule posts on social media, etc. could be relying on AI which you don't know about, haven't assessed so you don't understand, and crucially, haven't told your customers

about it hence you're not complying with the legal obligations based on you as a Controller. For this reason, clarifying with the supplier whether the tool you're intending to utilize features AI tools, is critical. You should also check if it allows feedback loops, i.e. the tool uses all the data you get from it, to continue learning and refining. Reports run on Microsoft Clarity, for example, do this. A good tell is normally the price of the tool – if it's free (like Microsoft Clarity), you are the product!

Marketing can be direct or indirect.

Where direct marketing uses personal information, it is covered by the UK data protection regime. This is set out in the Data Protection Act 2018 (DPA 2018) and the UK General Data Protection Regulation (UK GDPR).

Where direct marketing is carried out using electronic marketing messages (e.g. phone calls or electronic mail such as emails or text messages), it is also covered by the Privacy and Electronic Communications Regulations 2003 (as amended) (PECR). This means that any automated marketing aimed at individuals must comply with both pieces of legislation.

The ICO publish guidance on how to comply. If you don't follow this guidance, you may find it more difficult to show that your direct marketing complies with data protection law and PECR.
The ICO can take action against you if you send direct marketing or use personal information in a way that infringes the UK GDPR, DPA 2018 or PECR. However, as long as you can demonstrate that you found another way to comply with the law, you will not receive a penalty if you fail to adopt the Information Commissioner's

Office good practice recommendations.

Privacy and Electronic Communications Regulations (PECR)

So what exactly is PECR?

What is PECR?

The Privacy and Electronic Communications Regulations (PECR) sit alongside the Data Protection Act and the UK GDPR. They give people specific privacy rights in relation to electronic communications.

PECR applies to:

- Marketing by electronic communications (any information sent between particular parties over a phone line or internet connection)
- This includes phone calls, faxes, text messages, video messages, emails and internet messaging.
- It does not include generally available information such as the content of web pages or broadcast programming.

The Privacy and Electronic Communications Regulations (PECR) sit alongside the Data Protection Act and the UK GDPR. They give people specific privacy rights in relation to electronic communications.

PECR applies to any technology that stores information, or accesses information stored, on a subscriber's or user's 'terminal equipment'. This includes, but is not limited to:

- cookies;
- tracking pixels;
- link decoration and navigational tracking;
- web storage;
- fingerprinting techniques; and
- scripts and tags.

PECR applies to:

- Marketing by electronic communications (any information sent between particular parties over a phone line or internet connection)
- This includes phone calls, faxes, text messages, video messages, emails and internet messaging.

- It does not include generally available information such as the content of web pages or broadcast programming.

PECR also applies to electronic cookies
The rules on cookies are in regulation 6. The basic rule is that you must:
- tell people the cookies are there;
- explain what the cookies are doing and why; and
- get the person's consent to store a cookie on their device.

As long as you do this the first time you set cookies, you do not have to repeat it every time the same person visits your website. However, bear in mind that devices may be used by different people. If there is likely to be more than one user, you may want to consider repeating this process at suitable intervals.

PECR do not set out exactly what information you must provide or how to provide it – this is up to you. The only requirement is that it must be "clear and comprehensive" information about your purposes. You must explain the way the cookies (or other similar technologies) work and what you use them for, and the explanation must be clear and easily available. Users must be able to understand the potential consequences of allowing the cookies. You may need to make sure the language and level of detail are appropriate for your intended audience.

As cookies can capture personal details, the UK GDPR standard of consent must apply, and cookies must be covered by your privacy notice at the very least. To be valid, consent must be freely given, specific and informed. It must involve some form of unambiguous positive action – for example, ticking a box or clicking a link – and the person must fully understand that they are giving you consent.

Let's dive into the types of activity covered by PECR and what it says the rules are.

Telephone marketing

The rules on live marketing calls are in Regulation 21, 21A and 21B. In short, you must not make unsolicited live calls:

- to anyone who has told you they don't want your calls;
- to any number registered with the Telephone Preference Service (TPS) or Corporate TPS (CTPS), unless the person has specifically consented to your calls – even if they are an existing customer (unless the call is in relation to pension schemes and you meet a strict criteria, we'll cover shortly);
- for the purpose of claims management services, unless the person has specifically consented to your calls; or
- in relation to pension schemes unless you are a trustee or manager of a pension scheme or a firm authorised by the Financial Conduct Authority, and the person you are calling has specifically consented to your calls or your relationship with the individual meets a strict criteria.

You must always say who is calling, allow your number (or an alternative contact

number) to be displayed to the person receiving the call, and provide a contact address or freephone number if asked.

You can call any individual who has specifically consented to receive marketing calls from you, for example, by ticking an opt-in box.
You can also make live calls without consent to a number if it is not listed on the TPS, but only if that person hasn't objected to your calls in the past and you are not marketing claims management services.
In practice, this means you will need to screen most call lists against the TPS register. You will also need to keep your own 'do not call' list of people who object or opt out, and screen against that as well.

In general, you cannot make live marketing calls unless your relationship with the individual meets the following criteria:

- you have an existing customer relationship with the person you are calling;
- they might reasonably expect such a call from you; and
- you gave them a chance to opt-out of such calls when you collected their details and in every message you send them.

Electronic mail marketing
The rules on electronic mail marketing are in regulation 22. In short, you must not send electronic mail marketing to individuals, unless:

- they have specifically consented to electronic mail from you; or
- they are an existing customer who bought (or negotiated to buy) a similar product or service from you in the past, and you gave them a simple way to opt out both when you first collected their details and in every message you have sent.

You must not disguise or conceal your identity, and you must provide a valid contact address so they can opt out or unsubscribe.

This same rule applies to emails, texts, picture messages, video messages, voicemails, direct messages via social media or any similar message that is stored electronically.
The term 'electronic mail' has an intentionally broad meaning that includes new forms of messaging.

Mailing lists
You may want to compile your own in-house marketing list using details of people who have bought goods or services in the past, or who have registered on your website or made an enquiry. However, you should not assume that everyone is happy to receive marketing just because they have provided their contact

details.

You should make it clear upfront that you intend to use their details for marketing purposes. The best way to get clear consent for your marketing is to provide opt-in boxes that specify the type of messages you plan to send (eg by email, by text, by phone, by fax, by recorded call).

You should record when and how you got consent, and what type of messages it covers. If possible, you should also record whether the customer is an individual or a company, as different rules apply. If this is not clear, assume they are an individual.

Not everything you want to do will be considered direct marketing. But it is important to check if it is, so you can comply with all the relevant rules.

Direct marketing includes promoting your aims and ideals, as well as advertising your products or services. This means it includes fundraising and campaigning. Direct marketing is not just about sending messages. It can include activities that lead up to, enable or support you sending direct marketing (such as targeting and profiling).

Marketing is not "directed to" if it is indiscriminate blanket marketing. For example:

- leaflets delivered to every house in an area;
- magazine inserts;
- online adverts shown to everyone who views a website; or
- an advertising post on social media that is broadcast to all followers of the account or all users of the platform.

However, simply removing someone's name from the marketing material doesn't stop it from still being directed to that person.

Plan direct marketing

Planning your direct marketing before you start means that you can make sure it complies with the law.

It is important to think about:

1. Why is it important to plan our direct marketing activities?
2. what type of information you want to use;
3. what your data protection reason ("lawful basis") will be;
4. how you will ensure the information is accurate and not kept for longer than you need it.

Planning your direct marketing before you start means that you can make sure it complies with the law.

There are several things the law tells you you **MUST** do. These include:

You **must** take a 'data protection by design' approach when planning your direct marketing campaign or activity. For example, you **should** consider:

- what type of information you want to use (e.g. is it personal information, special category data or children's information?);
- what direct marketing activity you want to use the information for;
- who is responsible for compliance when you work with others;
- what data protection reason ("lawful basis") applies to your activity; and
- how will you ensure the information is accurate and not kept longer than you need it.

You **must** also be aware of whether any additional rules apply to the information you want to use or to the activity you want to carry out. You **must** be clear which legislation applies to your direct marketing activities so you can follow all the relevant rules. In some cases, only data protection law or only PECR will apply,

but in other circumstances all may apply.

You **must** have a valid data protection reason, if you want to use people's information for your direct marketing activity (known as a "lawful basis"). You **must** choose which is the most appropriate, depending on your direct marketing activity, the context and your relationship with the person. In general, consent and legitimate interests are the two lawful bases most likely to apply to your direct marketing.

You **must** consider if PECR applies to your direct marketing activity. It applies if you want to send direct marketing messages by phone call, electronic mail (eg emails and texts) or use cookies and similar technologies for online advertising.

You **must** ensure that you accurately record people's information for direct marketing. For example, you **should** accurately record:

- the information you have been provided with (eg contact details);
- the source of that information;
- which methods of direct marketing people have consented to;
- any objections, opt-outs, or withdrawals of consent; and
- people's details on suppression lists (see What are direct marketing suppression lists?).

The Information Commissioner's Office guidance also advises that you **SHOULD** do some things unless there is a good reason not to. For example:

You **should** plan your direct marketing activity before you start so that you can build-in data protection and PECR compliance. It is hard to retrofit legal requirements once you have started your activity and it may be costly. You may find that not planning properly means you are infringing the law. This may harm your reputation and your relationship with people.

You **should** think about what type of information you want to use for your direct marketing activity before you start. This will help you know which rules apply. For example, if you want to use personal information, then you **must** comply with data protection law. Personal information can simply be someone's name and address but it is also broader. It covers distinguishing between people and singling them out. For example, in the direct marketing context, personal information covers:

- a person's email address;
- a business email address if this identifies a person (eg lastname@company.com); and

- online identifiers such as cookie IDs, IP addresses or advertising IDs.

If you want to use contact details, such as a phone number or electronic mail address (e.g. email address), then PECR applies (as well as data protection law if your marketing involves using personal information).

Profiling for marketing purposes

Profiling can simply be realising that your customer likes a to buy a particular type of product from you and tailoring your marketing accordingly.

But sometimes it can be more intrusive, for example due to the type of information used (eg health, financial), or the amount being gathered on someone.

If you're thinking about profiling for marketing, you must do the following:

- **Be fair and tell people what you want to do**.
- **Ensure you have a lawful basis**.
- **Own your compliance.**

There are a number of ways that you may decide to seek contact details and additional information to use for your direct marketing, including from:

- the people who buy your products and services or support your cause (ie people you have a direct relationship with);
- third parties who sell or rent lists of contact details or who can provide additional information on your customers; or
- publicly available sources.

You may be seeking this information to:

- reach potential new customers (eg obtaining contact details for people you don't already have a relationship with);
- find new contact details for your existing customers (eg adding new contact channels for them); or
- profile your customers (eg analysing their behavioural characteristics to find out their preferences or predict their behaviour).

Whichever way you collect information or generate leads on potential or existing customers, you **must** ensure that what you want to do is fair, lawful and transparent. You **must** be open and honest.

So can you create profiles of people for direct marketing?
Profiling is where you look at people's interests, habits and behaviour, for example. Profiling for direct marketing often also involves predictions or assumptions about people. It can help you target your direct marketing messages to people who are more likely to buy your product or support your cause. It can also make your messages more relevant to the people that receive them.

Profiling can simply be realising that your customer likes a to buy a particular type of product from you and tailoring your marketing accordingly. But sometimes it can be more intrusive, for example due to the type of information used (eg health, financial), or the amount being gathered on someone.

If you're thinking about using profiling for your direct marketing it is important to do the following:

- **Be fair and tell people what you want to do**.
    - You **must** make sure the profiling is fair to people. For example, they are unlikely to anticipate you seeking to learn more about them and adding information from other sources to create a profile on them.
    - You **must** also tell people about your profiling and clearly explain to them what you will be doing. This includes if you are going to use third parties or public sources to expand the profile on them. You **must** also ensure the information you hold for the profile is accurate and not excessive.
- **Ensure you have a lawful basis**.
    - You **must** have a data protection reason ("lawful basis") for your profiling activity. (See How do we decide what our data protection reason ("lawful basis") is for direct marketing?)
    - If you are profiling people for direct marketing using their special categories of data, you are likely to need explicit consent. (See Can we use special category data for direct marketing?)
- **Own your compliance**
- You **must** be clear how your use of the information complies. For example:
- You **must** be able to demonstrate what your data protection reason ("lawful basis") is for using people's information that is being provided to you.
- If you're getting a list of potential new customers or supporters, you **should** check the information against your own suppression lists, so you don't contact anyone who has previously asked you not to (unless they have given you consent that overrides their previous objection).
- If you want to get more information on people, you **must** tell them that you want to do this.

- You **must** ensure that what you intend to do with the information is fair, reasonable and proportionate.
- Once you have obtained a list of potential customers or supporters, you **must** provide them with your own privacy information detailing anything they've not already been told.

Source: What do we need to tell people if we collect their information from other sources?)

Respect people's preferences

You **must** comply if someone exercises these rights.

People can:

- object to your direct marketing;
- opt-out or unsubscribe;
- withdraw their consent to your direct marketing; and
- ask you to delete their information.

Many people will be happy for you to use their information for direct marketing purposes, but some might not want you to do this, or they may change their mind.

It is important to respect people's preferences to maintain good relationships with your customers. It is also important because the law gives people rights about whether they want you to use their information for direct marketing.
You **must** comply if someone exercises these rights.
People can:

- object to your direct marketing;
- opt-out or unsubscribe;
- withdraw their consent to your direct marketing; and
- ask you to delete their information.

If someone objects, you **must** stop using their personal information for direct marketing. There are no reasons that you can use to refuse their objection. This right covers any use of people's information for direct marketing purposes, including profiling. For example, using people's information to try to infer what products or services people in a particular geographical location might be

interested in or disclosing their information to third parties for direct marketing purposes.

If someone opts out of your direct marketing, you **must** stop using their information for the direct marketing purposes that the opt-out covers. For example, you may be relying on the PECR soft opt-in to send direct marketing emails. If your customer uses the 'unsubscribe' link within your email to opt-out, you **must not** send them any further marketing emails.

Someone opting-out of receiving direct marketing works in the same way as if they had issued an objection to direct marketing on that channel. This is because they are making it clear that they don't wish to get your direct marketing. However, unlike an objection, an opt-out is more likely to cover a specific method of contact or a particular direct marketing activity, rather than being a general objection to all direct marketing purposes.

Although people may have initially been happy to consent to your direct marketing, they may change their mind. Data protection law and PECR allow people to withdraw their consent to your direct marketing. The key things to remember are:

- you **must** make it as easy for people to withdraw consent as it was to give it;
- if someone withdraws their consent you **must** stop the direct marketing that the consent covers immediately or as soon as possible; and
- if consent is withdrawn and this was your data protection reason ("lawful basis") for the direct marketing, you **must not** swap to a different basis to continue your direct marketing (this would be unfair).

People may ask you to delete or erase the information you hold about them. They have a specific data protection right to ask you to erase their information (also known as the right to be forgotten). This can include their information that you use for direct marketing purposes.
However, this right only applies in certain circumstances such as:

- you are using consent for the direct marketing and it is withdrawn;
- you no longer need their information for your direct marketing purpose; or
- someone objects to you using their information for direct marketing purposes.

You don't need to automatically treat withdrawals of consent or objections to direct marketing as an erasure request. However, in practice if someone withdraws their consent, you can no longer keep using their information for that purpose. Similarly, if someone objects to you using their information for direct marketing purposes, you **must** stop. Therefore, you are likely to need to delete that information (unless you need to keep a small amount for another reason,

such as on a suppression list).

Risk mitigation measures

Risk	Mitigation
Lawful basis and consent mapping	Document legal basis for each marketing use
Lack of documented accountability	Data Protection Impact Assessment completed before processing commences
Transparency and user controls	Clear notices - Explainable summaries of how modes influence offers or decisions Simple opt-outs
Segmentation safety checks	Test marketing segments for bias and disparate impact Apply fairness metrics and human sign-off before campaigns
Retention and purpose limits	Enforce strict retention schedules for telemetry and behavioural data Avoid repurposing training data
Security and monitoring	Apply access controls Apply anomaly detection Apply logging to detect exfiltration or misuse of data
Supplier governance	Require suppliers to demonstrate privacy-preserving practices Assess against and evidence compliance with UK GDPR Article 28

As you'll see, there is plenty of benefit to using AI, and marketing in your business. However, where personal data is involved or your marketing activity is electronic, you must risk assess the processes you want to put in place, and justify them.

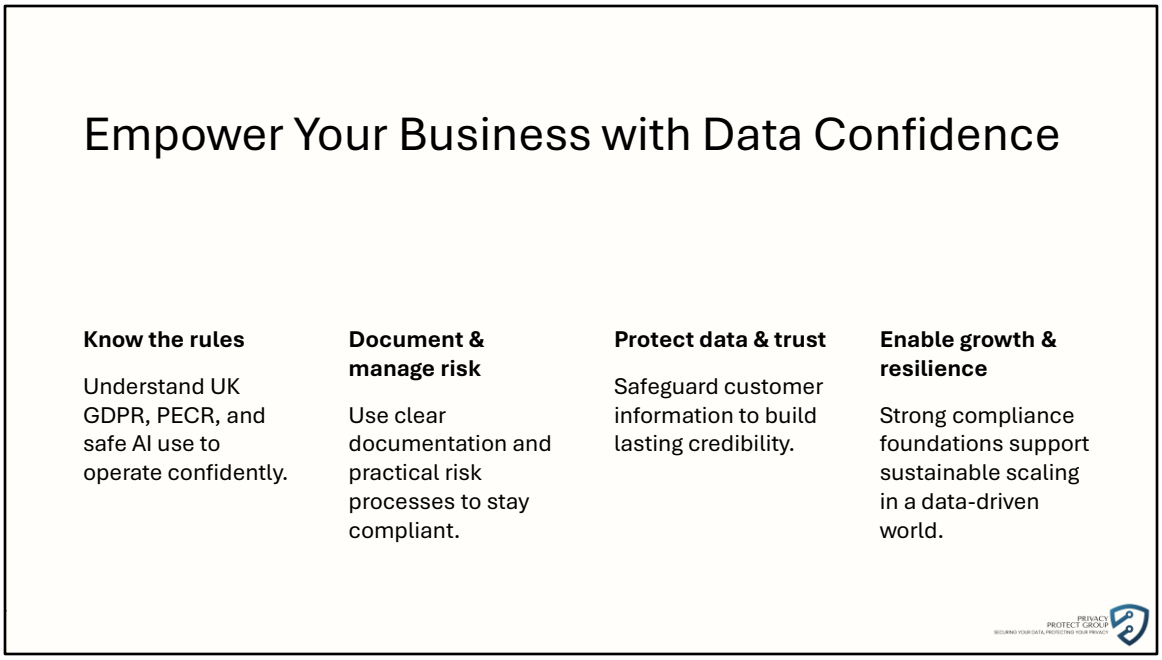
Depending on your risk appetite, risk mitigation for AI based marketing risks, for example, could look like those listed in the table.

Applying mitigations is about reducing any risks of non-compliance or negative impact to an acceptable level. There will be different ways to do so, and you can apply measures to either reduce the likelihood of something going wrong, or the impact should it go wrong. You will also likely put in place both technical and softer, policy-based controls to ensure a proportionate and balanced approach. As long as your position is defensible, and you can justify and evidence that the approach is compliant with the legislation, you will be in a good position should your practices ever be queried by a data subject or the regulator.

FYI only
Source:
ai-privacy-risks-and-mitigations-in-llms.pdf

Documents for Compliance

document	
DPIA	A DPIA is a process designed to help you systematically analyse, identify and minimise the data protection risks of a project or plan.
GDPR documentation controller	Use this template to document the processing activities you undertake as a controller.
Ai and Data Protection risk toolkit	Practical support for organisations assessing the risks to individual rights and freedoms caused by their own AI systems.
Ai tracker	Once you have read each toolkit, use our audit trackers to assess your procedures and the risks to people's personal information. You can record more detail and create an action plan to track your progress over time.
Accountability toolkit tracker	This toolkit will help you better understand what you need to put in place for good corporate governance and how to achieve accountability in your organisation.
Record Management tracker	This toolkit will help you assess whether you have met the minimum standards for creating records and have effective mechanisms to locate and retrieve them.



In summary, understanding UK GDPR, PECR, and the safe use of new technologies like AI is essential small businesses to thrive.

By implementing clear documentation and risk management practices, you can confidently navigate compliance, protect your customers' data, and build trust.

This foundation will support your business's growth and resilience in a data-driven world.

Thank you!

What questions do you have?

And don't forget to reach out to get your fully-funded one hour of consultancy.